شناسایی و رتبه‌بندی عوامل ریسک رایانش ابری در سازمان‌های دولتی

نورمحمد یعقوبی[1] | حمیدرضا جعفری[2] | جواد شکوهی[3]

۱. دکتری مدیریت؛ دانشیار؛ دانشگاه سیستان و بلوچستان nm.yaghoubi@gmail.com

۲. [پدیدآور رابط] کارشناسی ارشد مدیریت فناوری اطلاعات؛ دانشگاه سیستان و بلوچستان jafari.itm@gmail.com

۳. دانشجوی دکتری مدیریت دولتی؛ دانشگاه سیستان و بلوچستان shokohe91@gmail.com

مقالهٔ پژوهشی

دریافت: ۱۳۹۳/۰۶/۱۶
پذیرش: ۱۳۹۳/۰۹/۱۶

دورهٔ ۳۰ شماره ۳
ص‌ص. ۷۵۹-۷۸۴

چکیده: با پیشرفت سریع فناوری‌های پردازشی و ذخیره‌سازی و موفقیت اینترنت، منابع رایانشی ارزان‌تر، قوی‌تر، و قابل دسترس‌تر از قبل شده‌اند. این روندِ فناوری تحقق یک مدل محاسباتی جدید به نام رایانش ابری را امکان‌پذیر ساخته است. اخیراً سازمان‌های دولتی شروع به استفاده از معماری، بسترها و برنامه‌های رایانش ابری جهت تحویل خدمات و برآورده‌ساختن نیازهای زیرمجموعهٔ خود کرده‌اند. با وجود مزایا و فرصت‌های بسیار فناوری رایانش ابری، ریسک‌های متعددی وجود دارند که سازمان های دولتی باید قبل از مهاجرت به سمت محیط ابری آنها را بشناسند. هدف از انجام این پژوهش، شناسایی و رتبه‌بندی عوامل ریسک رایانش ابری در سازمان‌های دولتی با استفاده از دیدگاه خبرگان فناوری اطلاعات می‌باشد. ابتدا، با مرور مقاله‌های کلیدی، لیست جامعی از ریسک ها استخراج و در دو دستهٔ محسوس و غیر محسوس طبقه‌بندی شدند. سپس، از ۶ نفر از خبرگان در خصوص این ریسک‌ها و تقسیم‌بندی آنها مصاحبه به عمل آمد و ۱۰ ریسک شناسایی شد. پس از آن، این ریسک‌ها با نظرسنجی از ۵۲ خبره و با کمک فرایند تحلیل سلسله‌مراتبی فازی رتبه‌بندی گردیدند. نتایج نشان می‌دهد که خبرگان، ریسک‌های نامحسوس را به‌عنوان مهم‌ترین ریسک‌ها در به‌کارگیری رایانش ابری در سازمان‌های دولتی شناسایی کرده‌اند. در این میان ریسک «محرمانگی داده» رتبهٔ نخست را به‌دست آورد.

کلیدواژه‌ها: رایانش ابری؛ سازمان‌های دولتی؛ عوامل ریسک؛ فرایند تحلیل سلسله‌مراتبی فازی

پژوهشنامهٔ پردازش و مدیریت اطلاعات
فصلنامه | علمی پژوهشی
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISA، ISC و Scopus
http://jipm.irandoc.ac.ir
پژوهشگاه علوم و فناوری اطلاعات ایران

۱. مقدمه

رایانش ابری اخیراً به‌عنوان پارادایم جدیدی برای میزبانی و ارائهٔ خدمات از طریق اینترنت مطرح شده است (Lian et al. 2013). اساس این پدیده بر این ایده استوار است که افراد و شرکت‌ها به‌جای اینکه محصولات مورد نیاز برای رایانش، ذخیره‌سازی و نیز نرم‌افزارهای مورد نیاز را خریداری کنند تا بتوانند در مواقعی از بخشی از امکانات آن استفاده نمایند، این موارد را به‌هنگام نیاز به‌صورت خدمات از طریق شبکه دریافت کرده و بر اساس میزان مورد نیاز بهای آن را می‌پردازند. همچنین، رایانش ابری قادر است منابع خود را هم‌زمان با تغییر تقاضای خدمات، به‌گونه‌ای انعطاف‌پذیر تغییر دهد. به این ترتیب، شرکت‌های عظیم که توانایی ایجاد زیرساخت‌های لازم و سرمایه‌گذاری‌های کافی را دارند، به فروش رایانش و قابلیت ذخیره و نرم‌افزار و سایر خدمات به‌صورت آنلاین خواهند پرداخت (Avram 2014). بر اساس تحقیقات مؤسسهٔ گارتنر، انتظار می‌رود سرمایه‌گذاری در رایانش ابری تا سال ۲۰۱۴ به ۱۵۰ میلیارد دلار و تا سال ۲۰۱۵ به ۲۲۰ میلیارد دلار برسد (همان). اخیراً سازمان‌های دولتی شروع به استفاده از معماری، بسترها و برنامه‌های رایانش ابری جهت تحویل خدمات و برآورده‌ساختن نیازهای زیرمجموعهٔ خودکرده‌اند (Paquette et al. 2010).

اگرچه مزایای بسیاری در استفاده از رایانش ابری گزارش شده است، ولی ریسک‌های بسیاری با پیاده‌سازی، مدیریت و استفاده از فناوری رایانش ابری همراه است. متفاوت از مدل محاسباتی سنتی که در آن کاربران بر ذخیرهٔ داده‌ها و محاسبات کنترل کامل دارند، در رایانش ابری لازم است که مدیریت فیزیکی داده‌ها و ماشین‌ها به ارائه‌دهندگان خدمات ابری محول شود. بنابراین، صحت و درستی ذخیرهٔ داده و محاسبات ممکن است به‌علت اینکه صاحبان داده بر امنیت داده‌شان کنترل ندارند، به خطر بیفتد (Wei et al. 2013). رایانش ابری، نابالغ بوده و هنوز برای استفادهٔ گسترده، خصوصاً برای استفادهٔ سازمان‌های با مأموریت حساس آماده نیست. برای مثال، بر اساس پیمایشی که «انجمن کنترل و بازرسی سیستم‌های اطلاعاتی»[1] در سال ۲۰۱۰ انجام داد، اعضای اقیانوسیه دریافتند که ۴۹ درصد از پاسخ‌دهندگان باور دارند که ریسک‌های رایانش ابری مهم‌تر از

1. Information Systems Audit and Control Association (ISACA)

مزایای آن است و ۳۰ درصد آنها، هیچ برنامه‌ای برای اینکه از رایانش ابری جهت پیشبرد خدمات مبتنی بر فناوری اطلاعات سازمان استفاده کنند، ندارند (Bannerman 2010). بر اساس تحقیق مؤسسهٔ دانشگاهی اینگرسول[1]، ۷۴ درصد مدیران فناوری اطلاعات اشاره کرده‌اند که امنیت به‌عنوان مانعی جهت حرکت به سمت مدل خدمات ابری به شمار می‌رود. هر چه بازار جهانی و کسب‌وکارها به سمت سیستم‌های ابری حرکت می‌کنند، مباحث محرمانگی و ریسک‌ها برجسته‌تر می‌شود (Colt 2011). ریسک‌های فراوانی در محیط استفاده از رایانش ابری وجود دارند که می‌توانند اثرات جبران‌ناپذیری بر اطلاعات و خدمات پشتیبانی‌شده توسط این فناوری بگذارند و نیز چالش‌هایی را برای مدیریت فناوری اطلاعات ایجاد کنند. توانایی سازمان‌ها برای مدیریت‌کردن این ریسک‌ها در موفقیت رایانش ابری تعیین‌کننده و کلیدی خواهد بود. بنابراین، باید قبل از هرگونه فعالیت در زمینهٔ رایانش ابری، مسائل مربوط به امنیت، محرمانگی، پیروی از مقررات و میزبانی ریسک‌های دیگر به‌دقت مورد بررسی قرار گیرند.

مطالعاتی که تاکنون در رابطه با ریسک و چالش‌های امنیتیِ به‌کارگیری رایانش ابری انجام شده، اغلب از نوع کیفی بوده و فقط به بیان کلی ریسک‌ها و تحلیل‌ها و راه‌حل‌های کاهش آنها می‌پردازند. به‌عنوان نمونه، ژو و همکارانش راجع به اینکه ارائه‌دهندگان خدمات ابری با موضوعات امنیتی ابر، مثل دسترس‌پذیری، محرمانگی، جامعیت داده، کنترل و بازرسی چگونه برخورد می‌کنند، بحث کرده‌اند (Zhou et al. 2010). در مقاله‌ای دیگر سوباشینی و کاویتا ریسک‌ها را بر اساس مدل‌های سه گانهٔ رایانش ابری (نرم‌افزار، زیرساخت، و بستر) تقسیم نمودند و به تحلیل بیشتر ریسک‌های مدل نرم‌افزار به‌عنوان خدمت پرداختند (Subashini & Kavitha 2011). برخی از مسائل حقوقی و قانونی مربوط به مشتریان و ارائه‌دهندگان خدمات ابری جهت امنیت دادهٔ ذخیره‌شده در ابر را می‌توان در مقالهٔ کافمن مشاهده کرد (Kaufman 2009).

هدف اصلی این تحقیق، ارائهٔ چارچوبی جهت شناسایی و رتبه‌بندی عوامل ریسک رایانش ابری در سازمان‌های دولتی می‌باشد. با توجه به نبودِ چنین پژوهشی در کشور در ارتباط با شناسایی و رتبه‌بندی عوامل ریسک رایانش ابری و با توجه به توسعه و توجه

1. Ingersoll District Collegiate Institute (IDCI)

روزافزون سازمان‌های دولتی به حوزهٔ رایانش ابری، ضرورت چنین پژوهشی احساس می‌شود و تحقیق پیش رو نیز به این موضوع می‌پردازد. بنابراین، سؤالاتی که این تحقیق به دنبال پاسخ‌گویی آنهاست، عبارت‌اند از:

۱. عوامل ریسک رایانش ابری در سازمان‌های دولتی کدامند؟
۲. رتبه‌بندی این عوامل به چه صورت می‌باشد؟

در این پژوهش ابتدا عوامل ریسک رایانش ابری، با استفاده از ادبیات تحقیق، استخراج و در دو دستهٔ محسوس و غیرمحسوس طبقه‌بندی شدند. سپس، از ۶ نفر از خبرگان در خصوص این عوامل و تقسیم‌بندی آنها جهت تطبیق آنها در سازمان‌های دولتی مصاحبه به عمل آمد و ۱۰ عامل شناسایی شده و در دسته ها قرار گرفتند. پس از آن، این ریسک‌ها با نظرسنجی از ۵۲ نفر از خبرگان و با کمک فرایند تحلیل سلسله‌مراتبی فازی رتبه‌بندی گردیدند.

۲. مبانی نظری

۲-۱. رایانش ابری

رایانش ابری به ظهور مدلی از محاسبات برمی‌گردد، به‌طوری که ماشین‌هایی در مرکز داده‌های بزرگ می‌توانند به‌صورت پویا مستقرشده، پیکربندی، و پیکربندی مجدد شوند تا خدمات را به روشی مقیاس‌پذیر برای نیازهای مختلف، از تحقیقات علمی گرفته تا به اشتراک‌گذاری فیلم و پست الکترونیکی، تحویل دهند (Wyld 2009).

مؤسسهٔ ملی استانداردها و فناوری آمریکا[1] رایانش ابری را این‌گونه تعریف می‌کند: «رایانش ابری مدلی است برای فراهم‌کردن دسترسی آسان از طریق شبکه و بر اساس تقاضای کاربر به مجموعه‌ای از منابع رایانشی قابل تغییر و پیکربندی (مثل شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) که این دسترسی بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم فراهم‌کنندهٔ سرویس، به‌سرعت فراهم شده یا آزاد (رها) گردد» (Shahzad 2014). بر مبنای این تعریف و همان‌طور که در شکل ۱ مشاهده می‌شود، مدل رایانش ابری از پنج ویژگی مهم، سه مدل خدمات و چهار

1. National Institute of Standards and Technology (NIST)

شکل ۱ مشاهده می‌شود، مدل رایانش ابری از پنج ویژگی مهم، سه مدل خدمات و چهار مدل به‌کارگیری تشکیل شده است.

شکل ۱. مدل رایانش ابری NIST

ویژگی‌های توصیف‌شده عبارت‌اند از: «سرویس‌دهی بر اساس تقاضا»[1]، «دسترسی به شبکهٔ گسترده»[2]، «ادغام منابع»[3]، «قابلیت انعطاف سریع»[4] و« خدماتی که از لحاظ کمی کمی محاسبه شده‌اند»[5] (Shahzad 2014). «سرویس‌دهی بر اساس تقاضا» بیان‌کنندهٔ این است که کاربر می‌تواند از منابع رایانشی، بر اساس تقاضای خود و بدون تعامل با تأمین‌کننده استفاده کند. «دسترسی به شبکهٔ گسترده» به معنی تحویل تمامی خدمات و قابلیت‌های رایانش ابری از طریق شبکه می‌باشد. «ادغام منابع» عبارت است از گردآوری منابع ذخیره‌سازی، پردازشی، حافظه، پهنای باند و غیره برای ارائهٔ خدمات به مشتریان متعدد. «قابلیت انعطاف» سریع نشان می‌دهد که مقیاس منابع به‌طور خودکار و انعطاف‌پذیر و بر اساس تقاضای کاربران، بالا و پایین می‌شود و در نهایت، «خدماتی که از لحاظ کمی

1. on-demand self-service
2. broad network access
3. resource pooling
4. rapid elasticity
5. measured service

اندازه‌گیری پرداخت به ازای استفاده، به‌طور خودکار کنترل و بهینه‌سازی می‌کنند.

سه مدل خدمات عبارت‌اند از: «زیرساخت به‌عنوان خدمت»[1]، «بسترهای نرم‌افزاری به‌عنوان خدمت»[2] و «نرم‌افزار به‌عنوان خدمت»[3] (Mell and Grance 2011).

مدل «زیرساخت به‌عنوان خدمت»، به معنی دریافت خدمات زیرساختی از طریق ابر است و اشاره به تجهیزاتی دارد که توسط شرکت ارائه‌دهنده مدیریت می‌شود. در مدل «بستر نرم‌افزاری به‌عنوان خدمت»، کل بستر رایانشی یعنی سیستم‌عامل و سرویس‌های مرتبط در قالب خدمتی واحد ارائه می‌گردد. در مدل «نرم‌افزار به‌عنوان خدمت»، کاربران این امکان را می‌یابند تا از نرم‌افزارهای موجود در ابر که توسط خود ابر راه‌اندازی می‌شوند، استفاده کنند و نیازی به خرید، نصب یا اجرای آنها در کامپیوترهای شخصی نیست (Sultan 2011).

بر طبق تعریف مؤسسهٔ ملی استانداردهای فناوری آمریکا، چهار مدل به‌کارگیری رایانش ابری عبارت‌اند از: «ابر خصوصی»،[4] «ابر جمعی»،[5] «ابر عمومی»،[6] و «ابر پیوندی»[7] (Mell and Grance 2011).

زیرساخت «ابر خصوصی» به‌طور خاص برای سازمانی به‌کار می‌رود که متعلق به همان سازمان است و توسط خود آن مدیریت و هدایت می‌شود. «ابر جمعی» توسط چندین سازمان، کنترل و به اشتراک گذاشته می‌شود و برای پاسخ‌گویی به نیاز خاص جمعی از سازمان‌ها که دارای اشتراکاتی هستند، تدارک دیده می‌شود. در «ابر عمومی» منابع رایانشی از جمله ذخیره‌سازی و برنامه‌های کاربردی توسط ارائه‌دهندهٔ خدمات از طریق برنامه‌ها یا خدمات تحت وب در دسترس چندین مشتری قرار می‌گیرد. «ابر پیوندی» حاصل ترکیب‌شدن دو یا چند نوع ابر مشخص ذکرشده با یکدیگر است که توسط فناوری‌هایی که استانداردسازی‌ها و سازگاری‌های لازم را انجام می‌دهند، اطلاعات را میان خود ردوبدل می‌کنند (Carroll et al. 2011).

---

1. infrastructure as a service (IaaS)
2. platform as a service (PaaS)
3. software as a Service (Saas)
4. private cloud
5. community cloud
6. public cloud
7. hybrid cloud

رایانش ابری می‌تواند شیوهٔ دسترسی و استفادهٔ سازمان‌ها به محصولات و خدمات فاوا[1] را تغییر دهد. سازمان‌ها به‌جای مالکیت و مدیریت محصولات یا خدمات فناوری اطلاعات و ارتباطات و یا استفاده از رویکرد برون‌سپاری سنتی که در آن سخت‌افزار، نرم‌افزار و خدمات پشتیبانی به‌طور اختصاصی برای سازمان تهیه می‌شود، با به‌کارگیری خدمات رایانش ابری می‌توانند نیازهای فاوای خود را با استفاده از یک مدل انعطاف‌پذیر، مبتنی بر تقاضا، و مقیاس‌پذیر توسط تأمین‌کنندهٔ خدمات ابری فراهم کنند (Craig et al. 2009).

به‌طور کلی، از جمله مزایای رایانش ابری می‌توان به کاهش هزینه، مقیاس‌پذیری، ذخیرهٔ داده، کارایی و قابلیت اطمینان و به‌اشتراک‌گذاری منابع اشاره نمود. جدول شماره ۱ به چند نمونه از مزایای مهم استفادهٔ سازمان‌های دولتی از فناوری رایانش ابری اشاره می‌کند.

جدول ۱. مزایای مهم استفادهٔ سازمان‌های دولتی از فناوری رایانش ابری (Craig et al. 2009)

مزایا	توضیحات
صرفه‌جویی در هزینه‌ها	سازمان‌ها می‌توانند هزینه‌های سرمایه‌ای فاوا را کاهش داده یا حذف کنند و هزینه‌های عملیاتی خود را با پرداخت خدماتی که استفاده می‌کنند و به‌طور بالقوه با تعدیل یا نقل و انتقال کارکنان فاوا کاهش دهند.
پیاده‌سازی آسان	سازمان‌ها بدون نیاز به خرید سخت‌افزار، نرم‌افزار یا خدمات پیاده‌سازی می‌توانند رایانش ابری را در سریع‌ترین زمان ممکن به کار گیرند.
انعطاف‌پذیری	رایانش ابری در انطباق منابع فاوا با وظایف سازمان‌ها نسبت به روش‌های رایانشی گذشته، انعطاف‌پذیر می‌باشد. رایانش ابری همچنین می‌تواند تحرک و پویایی کارکنان را با دسترسی آنها به اطلاعات و برنامه‌های کاربردی سازمانی در طیفی وسیع از مکان‌ها یا دستگاه‌ها افزایش دهد.
مقیاس‌پذیری	سازمان‌ها با استفاده از رایانش ابری به همان میزان که از خدمات ابر استفاده کرده‌اند، هزینه پرداخت می‌کنند.

۱. فناوری اطلاعات و ارتباطات

مزایا	توضیحات
نقل و انتقال کارکنان فناوری اطلاعات	با کاهش یا حذف به‌روزرسانی مداوم سرورها و دیگر موضوعات رایانشی و با کاهش هزینه‌های مالی و زمانی جهت توسعهٔ برنامه‌های کاربردی، سازمان‌ها می‌توانند از کارکنان فناوری اطلاعات در کارهای باارزش‌تر استفاده نمایند.
تمرکز بر قابلیت‌های اصلی	مسلماً اکثر سازمان‌ها توانایی اداره‌کردن مرکز داده‌ها و توسعه و مدیریت برنامه‌های کاربردی را ندارند. رایانش ابری می‌تواند آن وظایف را از دوش سازمان‌ها بردارد و به‌گونه‌ای آسان انجام دهد و به سازمان‌ها اجازه دهد تا توجه خود را به موضوعات مهمی مانند توسعهٔ خط مشی‌ها و طراحی و تحویل خدمات دولتی معطوف کنند.
توسعهٔ پایدار	تأمین‌کنندگان خدمات ابر می‌توانند با استفاده از صرفه‌جویی‌های ناشی از مقیاس و توان خود جهت مدیریت کارآمد منابع رایانشی، انرژی و منابع دیگر را بسیار کمتر از اپراتورهای مرکز دادهٔ سنتی مصرف کنند. اکثر مرکز داده‌ها از لحاظ مصرف انرژی و به‌کارگیری دارایی‌های ناکارآمد با توجه به مسائل محیطی و اقتصادی کارایی لازم را ندارند.

۲-۲. عوامل ریسک رایانش ابری

آورام مزایا و چالش‌هایی را که باید هنگام تصمیم‌گیری در مورد استفاده از رایانش ابری توسط سازمان‌ها مورد توجه قرار گیرند، از نقطه‌نظر سازمان‌ها تحلیل کرده است. این چالش‌ها عبارت‌اند از: امنیت و محرمانگی، اتصال و دسترسی آزاد، قابلیت اطمینان، قابلیت همکاری، ارزش اقتصادی، تغییر در فناوری اطلاعات سازمان، و مسائل سیاسی مربوط به مرزهای جهانی (Avram 2014).

در مقاله‌ای دیگر، دوهرتی و همکاران، ریسک‌های اتخاذ رایانش ابری را به ریسک‌های مربوط به امنیت، فقدان استاندارد، وابستگی به فروشنده، مجوز نرم‌افزار، سطح پروژه، بازگشت سرمایه، اتصال، توافق، اعتماد و اعتبار ارائه‌کنندگان خدمات، و دسترس‌پذیری تقسیم‌بندی کرده و در ادامه، به بیان چارچوب بلوغ قابلیت فناوری اطلاعات[1]، به‌عنوان ابزاری مؤثر جهت ارزیابی آمادگی سازمان‌ها در مهاجرت به سمت محیط ابری و قادرساختن آنها در ایجاد نقشهٔ راه آینده می‌پردازند (Doherty et al. 2012).

1. Information Technology Capability Maturity Framework (IT-CMF)

برندر و مارکو مهم‌ترین ریسک‌های رایانش ابری از جمله امنیت اطلاعات، توافق قانونی، محافظت از داده‌ها، پشتیبانی تحقیقاتی، مکان داده، وابستگی به فروشنده، زیست‌پذیری بلندمدت، و دسترس‌پذیری و بازیابی را شرح داده و سپس بر ریسک‌ها و تحلیل‌های کنترلی شرکت‌های سوئیسی که از خدمات ابر عمومی استفاده می‌کنند، تمرکز نموده‌اند (Brender and Markov 2013).

پاکوئیتا و همکاران راجع به استفادهٔ رایج رایانش ابری در دولت ایالات متحدهٔ آمریکا و ریسک‌های محسوس و نامحسوس مرتبط با استفاده از آن بحث می‌کنند. در این مقاله، ریسک‌های محسوس شامل دسترسی، دسترس‌پذیری، زیرساخت، جامعیت و ریسک‌های نامحسوس شامل دسترسی و استفاده، قابلیت اعتماد، تداوم خدمات، مکانیزم‌های امنیتی، محرمانه‌بودن اطلاعات و حفظ حریم خصوصی، و حفظ اطلاعات و اسناد می‌باشند (Paquette et al. 2010).

اسکاتمن و همکاران، ریسک‌ها را به ۶ دستهٔ کلی شامل ریسک‌های کاربر، ریسک‌های سازمانی، ریسک‌های تأمین‌کنندهٔ شبکه، ریسک‌های ارائه‌دهندهٔ ابر، ریسک‌های محیطی و ریسک‌های حاکمیتی تقسیم کرده و در ادامه، به بیان ماتریسی جهت شناسایی و امتیازدهی ریسک‌ها توسط سازمان‌ها می‌پردازند (Schotman et al. 2013).

بانرمن با مرور مقاله‌های مرتبط با رایانش ابری بین سال‌های ۲۰۰۹ تا ۲۰۱۰، نود و نه ریسک مرتبط با به‌کارگیری رایانش ابری را جمع‌آوری نموده و سپس این ریسک‌ها را به ۱۰ دستهٔ کلیِ امنیت، وابستگی به فروشنده، کنترل، قانونی، خدمات، عملکرد، هزینه، حاکمیت، قابلیت‌ها، و صنعت تقسیم‌بندی می‌کند و در ادامه، مقایسه و تحلیل‌هایی را در ارتباط با ریسک‌هایی که از مقالات استخراج کرده، انجام می‌دهد (Bannerman 2010).

بنابراین، با توجه به موارد اشاره‌شده می‌توان مطالعات منتخب در زمینهٔ ریسک‌های مرتبط با به‌کارگیری رایانش ابری را برابر جدول شماره ۲ نشان داد.

جدول ۲. مطالعات منتخب در زمینهٔ ریسک‌های مرتبط با به‌کارگیری رایانش ابری

ریسک‌های شناسایی‌شده	مراجع
دسترسی، دسترس‌پذیری، زیرساخت، جامعیت داده، قابلیت اعتماد، تداوم خدمات، زیرساخت فیزیکی شبکه، محرمانگی داده، حفاظت از داده، حفظ حریم خصوصی	Paquette et al. 2010
دسترسی، جامعیت داده	Grobauer et al. 2011
دسترسی، وابستگی به فروشنده، قابلیت اعتماد، تغییر در فناوری اطلاعات سازمان، محرمانگی داده، مسائل سیاسی مربوط به مرزهای جهانی، بازگشت سرمایه	Avram 2014
امنیت، وابستگی به فروشنده، کنترل، قانونی، خدمات، عملکرد، هزینه، حاکمیت، قابلیت‌ها، صنعت	Bannerman 2010
دسترس‌پذیری، وابستگی به فروشنده، پشتیبانی تحقیقاتی، مکان داده	Heiser and Nicolett 2008
کاربر، سازمانی، تأمین‌کنندهٔ شبکه، ارائه‌دهندهٔ ابر، محیطی، ریسک‌های حاکمیتی	Schotman et al. 2013
دسترس‌پذیری، وابستگی به فروشنده، جامعیت داده، قابلیت اعتماد، پشتیبانی تحقیقاتی، فقدان استانداردها، مجوز نرم‌افزارها، اعتماد و اعتبار ارائه‌دهندگان خدمات، حفاظت از داده، حفظ حریم خصوصی	Doherty et al. 2012
دسترس‌پذیری، وابستگی به فروشنده، زیست‌پذیری بلندمدت فروشنده، پشتیبانی تحقیقاتی، تداوم خدمات، مکان داده، حفاظت از داده، توافق قانونی	Brender and Markov 2013
پشتیبانی تحقیقاتی، امنیت، جرائم رایانه‌ای	Cunningham 2009
محرمانگی داده، وابستگی به فروشنده، کنترل، عملکرد، امنیت، قابلیت اعتماد	Sultan 2010
مکانیزم ذخیره‌سازی	Tribhuwan et al. 2010
مکان داده، امنیت داده، دسترس‌پذیری داده	Mahmood 2011

۳. روش پژوهش

مطالعهٔ پیش رو تحقیقی توصیفی- پیمایشی با ماهیت کاربردی است. در این مطالعه، در پی ارائهٔ چارچوبی هستیم که بتواند مورد استفادهٔ سازمان‌های دولتی در به‌کارگیری رایانش ابری باشد.

برای این کار، ابتدا عوامل ریسک رایانش ابری با استفاده از مطالعات کتابخانه‌ای، مقالات و تحقیقات انجام‌شده در حوزهٔ رایانش ابری مورد شناسایی قرار گرفته و بر طبق ادبیات، به دو گروه محسوس و نامحسوس طبقه‌بندی شدند. سپس از ۶ نفر از خبرگانی که هر کدام بیش از پنج سال سابقه در زمینهٔ رایانش ابری دارند، در خصوص عوامل ریسک و طبقه‌بندی آنها مصاحبهٔ عمیق به‌عمل آمد. مصاحبه‌های عمیق فردی که به‌صورت رو در رو و نیمه‌ساخت‌یافته[1] است، عبارت است از طرح یک‌سری سؤال‌های از پیش تعیین‌شده و موضوعاتی خاص که به مصاحبه‌شونده این امکان را می‌دهد که در دامنهٔ وسیع‌تری به مصاحبه‌گر پاسخ دهد. هدف از انجام مصاحبه در این پژوهش، تطبیق عوامل ریسک مستخرج از ادبیات با سازمان‌های دولتی می‌باشد که در نهایت، با تغییرات گفته‌شده از جانب خبرگان، از میان جمعاً ۳۳ ریسک شناسایی‌شده (برابر جدول شماره ۲) بعد از حذف و یا ادغام ریسک‌های شناسایی‌شده، ۱۰ عامل ریسک (برابر جدول شماره ۳) مورد اجماع خبرگان قرار گرفت.

سپس، پرسشنامهٔ مقایسه‌های زوجی برای مقایسهٔ زوجی عوامل ریسک گفته‌شده طراحی شد و در اختیار ۶۲ نفر از خبرگان و اساتید دانشگاهی استان سیستان و بلوچستان در حوزهٔ فناوری اطلاعات و همچنین، مدیران فناوری اطلاعات سازمان‌ها و مراکز مهم استان از جمله سازمان صنعت، معدن و تجارت، سازمان مسکن و شهرسازی، سازمان آموزش و پرورش، سازمان آب و فاضلاب منطقه‌ای، دفتر فناوری اطلاعات استانداری، شرکت توزیع برق منطقه‌ای و سازمان جهاد کشاورزی قرار گرفت. لازم به ذکر است که همهٔ افراد ذکرشده در تدوین سند توسعهٔ فناوری اطلاعات استان نقش داشته‌اند. در نهایت،

1. semi-structured

از این تعداد، ۵۵ پرسشنامه دریافت شد و با بررسی به‌عمل آمده، ۵۲ پرسشنامه مورد استفاده قرار گرفت. سپس با کمک تکنیک «فرایند تحلیل سلسله‌مراتبی فازی»[1]، ریسک‌ها ریسک‌ها رتبه‌بندی شدند.

۳-۱. عوامل ریسک رایانش ابری در سازمان‌های دولتی

همان‌طور که در جدول شماره ۳ نشان داده شده، اجرای مرحلهٔ اول پژوهش به استخراج ۲ گروه از عوامل ریسک محسوس و نامحسوس منجر شده است. ریسک‌های محسوس، ریسک‌هایی هستند که کاربران می‌توانند به‌آسانی آنها را درک و لمس کنند. در حالی که ریسک‌های نامحسوس، ریسک‌هایی هستند که برای کاربران ناپیداست و کاربران آن را به‌آسانی درک نمی‌کنند و فقط تأمین‌کنندگان،آنها را می‌شناسند و مسئول تأمین آنها هستند.

برای ۲ گروه عوامل شناخته‌شده، در مجموع ۱۰ زیرگروه به‌دست آمده است.

جدول۳. عامل‌ها و زیرعامل‌های مرتبط با عوامل ریسک رایانش ابری در سازمان‌های دولتی

عامل‌ها	زیرعامل‌ها	تعاریف
ریسک‌های محسوس	دسترسی و دسترس‌پذیری[2]	* محافظت از داده‌های سازمان با مکانیزم شناسایی، تصدیق هویت و مجوز به کاربران جهت دسترسی به داده‌های سازمان (Sultan 2010)
		* دسترسی افراد به داده‌هایشان از هر مکان جغرافیایی به‌صورت سریع و آسان و بدون وقفه (Grobauer et al. 2011)
	فروشنده[3]	*تکلیف داده‌های مشتریان در صورت ورشکسته‌شدن یا خارج‌شدن مشتری از بازار (Heiser and Nicolett 2008)
		* وابستگی خریدار به فروشنده در تأمین خدمات مورد نیاز به‌طوری که تغییر فروشنده برای خریدار هزینه‌آور است (Bermbach et al. 2011)

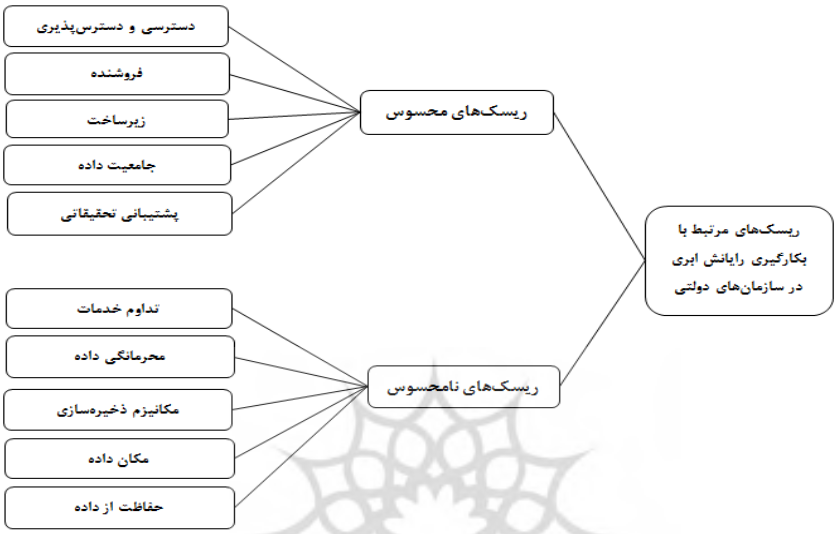
1. fuzzy analytic hierarchy process (FAHP)
2. access and availability
3. vendor

عامل‌ها	زیرعامل‌ها	تعاریف
	زیرساخت[1]	* انعطاف‌پذیری و مقیاس‌پذیری زیرساخت‌های ارائه‌شده توسط فروشنده (Paquette et al. 2010)
	جامعیت داده[2]	* کامل و بدون تغییر باقی‌ماندن داده‌ها در هنگام انتقال، پردازش و ذخیره در محیط ابری (Grobauer et al. 2011)
	پشتیبانی تحقیقاتی[3]	* امکان پیگیری و جمع‌آوری مدارک هنگام بروز هک یا کلاه‌برداری در سیستم‌های تحت محیط ابری (Cunningham 2009; Whitman and Mattord 2010)
ریسک‌های نامحسوس	تداوم خدمات[4]	* تحت تأثیر قرار نگرفتن وظایف سیستم و کاربران در صورت از کارافتادن یک خدمت یا فرایند در فرایندها یا خدماتی که پشت سر یکدیگر انجام می‌شوند (Paquette et al. 2010)
	محرمانگی داده[5]	انتقال دادهٔ مشتریان در محیط ابری با رمزگذاری (Sultan 2010)
	مکانیزم ذخیره‌سازی[6]	قابل تغییربودن فرمت ذخیره‌سازی به فرمت‌های دیگر در صورت تغییر فروشنده توسط مشتریان (Tribhuwan et al. 2010; Paquette et al. 2010)
	مکان داده[7]	اطلاع‌نداشتن مشتریان از محل دقیق ذخیرهٔ داده‌هایشان در محیط ابری (Sultan 2011; Mahmood 2011)
	حفاظت از داده[8]	نرم‌افزار یا سخت‌افزار مورد استفاده جهت تهیهٔ نسخهٔ پشتیبان از داده‌ها و محافظت از آنها در برابر حملات و نرم‌افزارهای مخرب توسط فروشندگان (Paquette et al. 2010)

در این مطالعه، مطابق شکل ۲، سطح اولِ درخت تصمیم، ریسک‌های مرتبط با

1. infrastructure
2. integrity of data
3. investigative support
4. service continuity
5. confidentiality of data
6. storage mechanism
7. location of data
8. protect data

رایانش ابری است که در سطح دوم به دو گروه و در سطح سوم بـه ۱۰ زیـرگـروه تقسـیم شده است.



شکل ۲. درخت سلسله‌مراتب تصمیم جهت رتبه‌بندی عوامل ریسک رایانش ابری در سازمان‌های دولتی

۳-۲. فرایند تحلیل سلسله‌مراتبی فازی

در هر تصمیم‌گیری، تصمیم‌گیرنده ممکن است با معیارهای مختلفی مواجه شـود. او در چنین شرایطی باید از روش‌های مطرح در این زمینه بهره جویـد. یکـی از ایـن روش‌هـا فرایند تحلیل سلسله‌مراتبی است. روش تحلیل سلسـله‌مراتبـی یکـی از معـروف‌تـرین فنـون تصمیم‌گیری چندمنظوره است که در سـال ۱۹۸۰ توسـط تومـاس سـاعتی ابـداع شـد. ایـن روش، هنگامی که عمل تصمیم‌گیری با چند گزینهٔ رقیـب و معیـار تصـمیم‌گیـری روبـه‌رو است، می‌تواند مورد استفاده قرار گیرد. اساس روش تحلیل سلسله‌مراتبی بر مقایسهٔ زوجـی یا دودویی گزینه‌ها و معیارهای تصمیم‌گیری است. برای چنین مقایسه‌ای نیاز به جمع‌آوری اطلاعات از تصمیم‌گیرندگان است و این امر به تصمیم‌گیرندگان این امکان را می‌دهد کـه تنها روی مقایسهٔ دو معیار یا گزینه تمرکز کنند (Saaty 1989).

برای برخورد با ابهام موجود در نظرات انسان‌ها، پروفسور لطفی‌زاده در سال ۱۹۶۵، نظریهٔ مجموعه‌های فازی را ارائه داد تا عدم قطعیتی را که به‌علت ابهام و عدم دقت در رویدادها ایجاد شده، به مدل درآورد. منطق فازی هدفش این است که اساسی را برای استدلال‌گری تقریبی با استفاده از تئوری مجموعهٔ فازی فراهم آورد. با توجه به اینکه تصمیم‌گیری انسان با مفاهیم نادقیق و مبهم همراه است، این مفاهیم بیشتر به‌صورت متغیرهای زبانی بیان می‌شوند (Kwong and Bai 2002).

فرایند تحلیل سلسله‌مراتبی فازی (FAHP) عبارت است از فازی‌سازی روش AHP کلاسیک با استفاده از اعداد و محاسبات فازی (آذر و فرجی ۱۳۸۹). این متدلوژی برای انتخاب یک گزینه به‌وسیلهٔ ادغام مفاهیم مجموعهٔ فازی و تجزیه و تحلیل ساختار سلسله‌مراتبی طراحی شد. ایدهٔ اساسی در AHP، گرفتن دانش خبرگان نسبت به پدیدهٔ مورد مطالعه است. کاربرد متدلوژی فازی به تصمیم‌گیرنده اجازه می‌دهد که داده‌های کمی و کیفی را در مدل تصمیم ادغام کند. با وجود این باید گفت که AHP سنتی قادر به انعکاس درست فرایندها نیست؛ به‌ویژه در شرایطی که مسائل تعریف نشده‌اند یا حل آنها مستلزم عدم اطمینان در داده است (Percin 2008). برای جبران این نقص، چانگ در سال ۱۹۹۲ روشی بسیار ساده را برای بسط فرایند تحلیل سلسله‌مراتبی به فضای فازی ارائه داد. این روش که مبتنی بر میانگین حسابی نظرات خبرگان و روش نرمالایز ساعتی و با استفاده از اعداد مثلثی فازی توسعه داده شده بود، مورد استقبال محققان قرارگرفت (زنجیرچی ۱۳۹۰، ۱۰۹).

مراحل انجام این روش به قرار زیر است (زنجیرچی ۱۳۹۰، ۱۱۱):

مرحلهٔ ۱، ترسیم درخت سلسله‌مراتبی: ابتدا ساختار سلسله‌مراتبی تصمیم با استفاده از سطوح هدف، معیار و زیرمعیارها ترسیم می‌شود.

مرحلهٔ ۲، تشکیل ماتریس مقایسات زوجی: با استفاده از نظر تصمیم‌گیرنده، ماتریس مقایسات با بهره‌گیری از اعداد فازی مثلثی بر اساس نظرات چندین تصمیم‌گیرنده تشکیل می‌گردد.

$$\tilde{c}_{ij} = (a_{ij}, b_{ij}, c_{ij})$$

مرحلهٔ ۳، محاسبهٔ میانگین حسابی نظرات: میانگین حسابی نظرات تصمیم‌گیرندگان به‌صورت ماتریس زیر محاسبه می‌گردد:

$$\tilde{s}_i = \sum_{j=1}^{n} \tilde{a}_{ij} \qquad i = 1,2,\dots,n \qquad \tilde{a}_{ij} = \frac{\sum_{k=1}^{p_{ij}} a_{ijk}}{p_{ij}} \qquad i,j = 1,2,\dots,n$$

مرحلهٔ ۴، محاسبهٔ مجموع عناصر سطر: مجموع عناصر سطرها را محاسبه کنید:

$$\tilde{A} = \begin{bmatrix} (1,1,1) & \tilde{a}_{12} & \tilde{a}_{1n} \\ \tilde{a}_{21} & (1,1,1) & \tilde{a}_{2n} \\ \vdots & \vdots & \vdots \\ \tilde{a}_{n1} & \tilde{a}_{n2} & (1,1,1) \end{bmatrix}$$

مرحلهٔ ۵، نرمالایزکردن اوزان سطرها: مجموع سطرها به شیوهٔ زیر نرمالایز می‌گردد:

$$\tilde{M}_i = \tilde{s}_i \otimes \left[\sum_{i=1}^{n} \tilde{s}_i\right]^{-1} \quad i = 1,2,\dots,n$$

در صورتی که $\tilde{s}_i$ را به‌صورت (li, mi, ui) نشان دهیم، رابطهٔ فوق به‌ترتیب زیر محاسبه می‌شود:

$$\tilde{M}_i = \left(\frac{l_i}{\sum_{i=1}^{n} u_i}, \frac{m_i}{\sum_{i=1}^{n} m_i}, \frac{u_i}{\sum_{i=1}^{n} l_i}\right)$$

مرحلهٔ ۶، تعیین درجهٔ احتمال بزرگتربودن: درجهٔ احتمال بزرگتربودن هر μi را نسبت به سایر μiها محاسبه و آن را d'(Ai) می‌نامیم. درجهٔ احتمال بزرگتربودن عدد مثلثی فازی μ2= (l2, m2, u2) نسبت به عدد مثلثی فازی μ1= (l1, m1, u1) برابر است با:

این رابطه را می‌توان مترادفاً به‌صورت زیر بیان کرد:

$$V(M_2 \geq M_1) = hgt(M_2 \cap M_1) = \mu_{M_2}(d)$$

$$= \begin{cases} 1 & m_2 \geq m_1 \text{ اگر} \\ 0 & l_2 \geq u_1 \text{ اگر} \\ \dfrac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)} & \text{در غیر اینصورت} \end{cases}$$

مرحلهٔ ۷، نرمالایزکردن: با نرمالایزکردن بردار وزن‌ها، وزن‌های نرمالایز به‌دست می‌آیند:

$$w = \left[\frac{d'(A_1)}{\sum_{i=1}^{n} d'(A_i)}, \frac{d'(A_2)}{\sum_{i=1}^{n} d'(A_i)}, \dots, \frac{d'(A_n)}{\sum_{i=1}^{n} d'(A_n)}\right]^T$$

وزن‌های فوق، وزن قطعی (غیرفازی) هستند. با تکرار این فرایند، اوزان تمامی ماتریس‌ها به‌دست می‌آید.

مرحلهٔ ۸، ترکیب اوزان: با ترکیب وزن‌های گزینه و معیارها، وزن‌های نهایی به‌دست می‌آید.

$$\tilde{U}_i = \sum_{j=1}^{n} \tilde{w}_i \tilde{r}_{ij} \qquad \forall i$$

۳-۳. محاسبات فرایند تحلیل سلسله‌مراتبی فازی با استفاده از روش چانگ

با استفاده از ساختار سلسله‌مراتبی (شکل ۲) و با دنبال‌کردن گام‌های فرایند فازی که در بالا به آن اشاره شد، ابتدا نظرات خبرگان (از طریق تبدیل عبارات کلامی به اعداد مثلثی فازی با توجه به جدول شماره ۴) تجمیع، و به‌منظور اطمینان از سازگاری ماتریس‌ها، نرخ ناسازگاری (جدول شمارهٔ ۵) مطابق روش گوگوس و بوچر (۱۹۹۸) محاسبه و سپس وزن هر یک از معیارهای سطوح دو و سه ساختار سلسله‌مراتبی محاسبه می‌شود.

به‌منظور کسب نظرات خبرگان در ماتریس مقایسه‌های زوجی از پرسشنامه استفاده شده است. پرسشنامه‌ها طوری طراحی گردیده بود که به پاسخ‌دهندگان این امکان را می‌داد تا با مقایسهٔ زوجی معیارها و زیرمعیارها در گروه خودشان، اهمیت هر یک از آنها را مشخص کنند. پس از جمع‌آوری پاسخ‌های خبرگان در قالب گویه‌های کلامی، بایستی پاسخ‌های مذکور به مقیاس فازی تبدیل شوند. مقیاس مورد استفاده در این پژوهش مقیاس فازی ۵ تایی (جدول شماره ۴) است که یانگ بر اساس مقیاس ساعتی پیشنهاد کرده است.

جدول ٤. طیف فازی و عبارت کلامی متناظر

کد	عبارات کلامی	عدد فازی
۱	اهمیت برابر	(۱,۱,۱)
۲	کمی مهم‌تر	(۱,۳,۵)
۳	نسبتاً مهم‌تر	(۳,۵,۷)
۴	مهم‌تر	(۵,۷,۹)
۵	بسیار مهم‌تر	(۷,۹,۹)

با توجه به شاخص‌های ناسازگاری CRg و CRm ارائه‌شده در جدول شماره ۵، در صورتی که هر دوی این شاخص‌ها کمتر از ۰/۱ بودند، ماتریس فازی سازگار است؛ در صورتی که هر دو بیشتر از ۰/۱ بودند، از تصمیم‌گیرنده تقاضا می‌شود تا در اولویت‌های ارائه‌شده تجدیدنظر نماید و در صورتی که تنها CRg یا CRm بیشتر از ۰/۱ بود، تصمیم‌گیرنده تجدید نظر در مقادیر میانی (حدود) قضاوت‌های فازی را انجام می‌دهد (زنجیرچی ۱۳۹۰، ۱۰۹).

جدول ۵. نرخ سازگاری ماتریس‌های تجمیع‌شده

سطوح ساختار سلسله‌مراتبی	عنوان ماتریس‌های تجمیع‌شده	نرخ ناسازگاری	
		CRg	CRm
سطح سوم	ماتریس تجمیع‌شدهٔ مقایسات زوجی ریسک‌های عامل محسوس	۰/۰۷	۰/۰۳
	ماتریس تجمیع‌شدهٔ مقایسات زوجی ریسک‌های عامل نامحسوس	۰/۰۴	۰/۰۲
سطح دوم	ماتریس تجمیع‌شدهٔ مقایسات زوجی ریسک‌های مرتبط با به‌کارگیری رایانش ابری در سازمان‌های دولتی	۰/۰۱	۰/۰۰

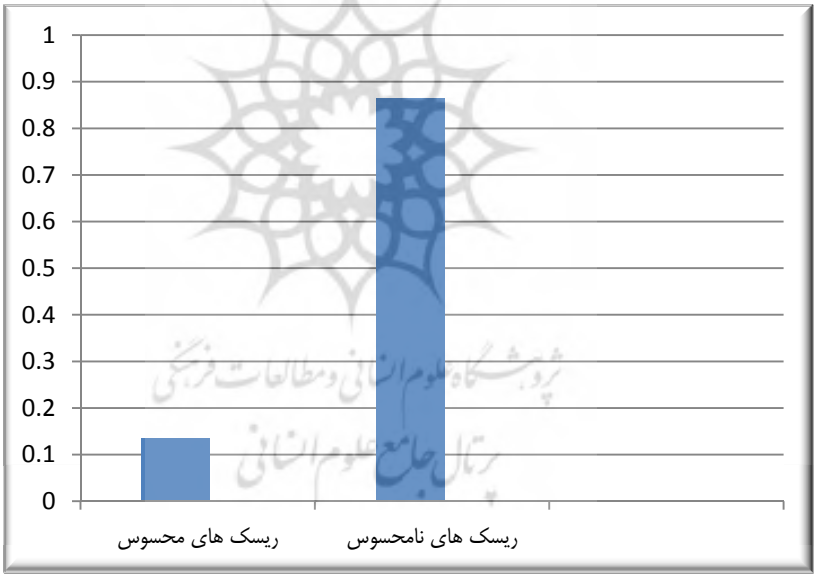
برای محاسبهٔ وزن نهایی هر یک ازمعیارها و زیرمعیارها که نشان‌دهندهٔ اهمیت آنها بر اساس نظر خبرگان است، لازم است در هر سطح درجهٔ ارجحیت هر یک از عوامل را نسبت به سایر عوامل مربوطه به‌دست آورده، سپس اوزان زیرمعیارهای سطح سوم را در وزن معیار مربوط به خود در سطح دوم، ضرب کنیم. جدول شماره ۷ وزن معیارهای سطح دوم و وزن زیرمعیارهای سطح سوم و وزن نهایی هر یک از زیرمعیارها را نشان می‌دهد.

جدول ۷. وزن معیارها و زیرمعیارها

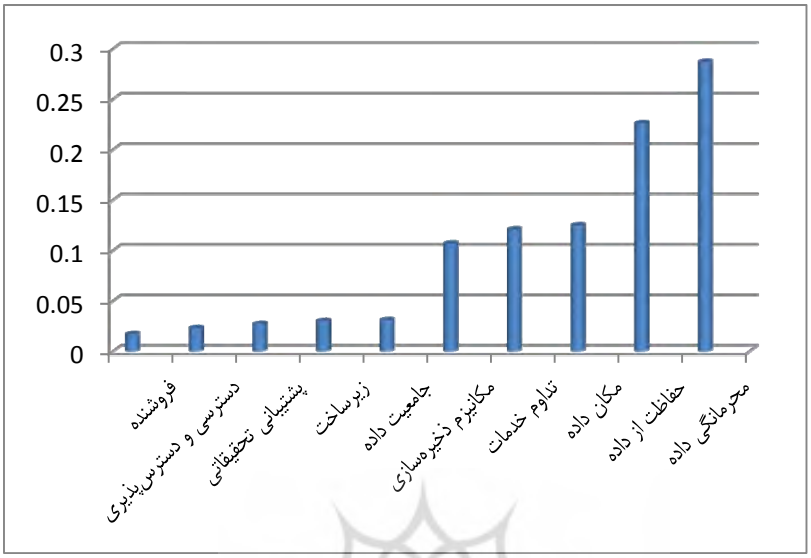
عامل	وزن	زیرعامل	وزن محلی	وزن نهایی
عوامل محسوس	۰/۱۳۵	دسترسی و دسترس‌پذیری	۰/۱۷۹	۰/۰۲۳
		فروشنده	۰/۱۳۴	۰/۰۱۷
		زیرساخت	۰/۲۳۵	۰/۰۳۰
		جامعیت داده	۰/۲۴۰	۰/۰۳۱
		پشتیبانی تحقیقاتی	۰/۲۰۹	۰/۰۲۷

عامل	وزن	زیرعامل	وزن محلی	وزن نهایی
عوامل نامحسوس	۰/۸۶۵	تداوم خدمات	۰/۱۴۰	۰/۱۲۱
		محرمانگی داده	۰/۳۳۰	۰/۲۸۷
		مکانیزم ذخیره‌سازی	۰/۱۲۴	۰/۱۰۷
		مکان داده	۰/۱۴۴	۰/۱۲۵
		حفاظت از داده	۰/۲۶۰	۰/۲۲۶

با توجه به اوزان نهایی معیارها و زیرمعیارها (جدول شماره ۷) می‌توان ریسک‌های مرتبط با به‌کارگیری رایانش ابری در سازمان‌های دولتی را رتبه‌بندی نمود. شکل شمارهٔ ۳ و ۴ نمودار میله‌ای اوزان نهایی مربوط به عامل‌ها و زیرعامل‌ها را نشان می‌دهد.



شکل۳. نمودار اوزان نهایی عامل‌ها



شکل ٤. نمودار اوزان نهایی زیرعامل‌ها

٤. نتایج و یافته‌ها

در این مقاله به شناسایی عوامل ریسک رایانش ابری و تعیین میزان اهمیت آنها پرداخته شد. اگرچه رایانش ابری برای سازمان‌ها مزایای بسیاری دارد، اما مدیران نباید ریسک‌های موجود در آن را نادیده بگیرند. بنابراین، مقولهٔ مدیریت ریسک در حیطهٔ پروژه‌های رایانش ابری اهمیت بسیاری دارد. بنا بر نظر بوهم، مدیریت ریسک فرایندی است که شامل دو فاز اصلی است: فاز تخمین ریسک (شامل شناسایی، تحلیل و اولویت‌بندی) و فاز کنترل ریسک (شامل برنامه‌ریزی مدیریت ریسک، برنامه‌ریزی نظارت ریسک و اقدامات اصلاحی). این پژوهش فاز اول فرایند مدیریت ریسک را تا حد زیادی پوشش داده و کلیهٔ ریسک‌های مرتبط با به‌کارگیری رایانش ابری و ساختار آنها را در مقاله‌ها بررسی و چارچوب جدیدی متناسب با سازمان‌های دولتی ارائه‌کرده است. در این پژوهش از روش فرایند تحلیل سلسله‌مراتبی فازی برای رتبه‌بندی ریسک‌های مرتبط با به‌کارگیری رایانش ابری در سازمان‌های دولتی با بهره‌گیری از نظر ۵۲ خبرهٔ فناوری اطلاعات و مدیران فناوری اطلاعات سازمان‌های دولتی استان سیستان و بلوچستان استفاده

شده است. چارچوب پیشنهادی این پژوهش، می‌تواند شناخت مناسبی از ریسک‌های مرتبط با به‌کارگیری این فناوری، اهمیت، و اولویت ریسک‌ها را به سازمان‌هایی که تصمیم به استفاده از فناوری رایانش ابری گرفته‌اند، نشان دهد. همچنین، این چارچوب به سازمان‌های دولتی کمک می‌کند که قبل از مهاجرت به سمت محیط ابری، آن ریسک‌ها را بشناسند و در نظر بگیرند. شناسایی ریسک‌ها و مدیریت آنها می‌تواند محرمانگی، یکپارچگی و در دسترس‌بودن داده‌ها را تضمین نماید.

گفتنی است در هیچ‌یک از مقاله‌های مرورشده، برای شناسایی عوامل ریسک، علاوه بر استفاده از ادبیات تحقیق از نظر خبرگان استفاده نشده و این عوامل نیز رتبه‌بندی نشده‌اند. در جدول شماره ۸، نتایج پژوهش حاضر با پژوهش‌های گذشته مقایسه شده است.

جدول ۸. مقایسهٔ تحقیق حاضر با تحقیقات گذشته

معیار / مراجع	شناسایی و تقسیم‌بندی ریسک‌ها: ادبیات موضوع	شناسایی و تقسیم‌بندی ریسک‌ها: دیدگاه خبرگان	ارائهٔ تقسیم‌بندی ریسک‌ها	بخش دولتی	بخش خصوصی	اولویت‌بندی ریسک‌ها
Paquette et al. 2010	✓		✓	✓		
Avram 2014	✓					
Brender and Markov 2013	✓				✓	
Craig et al. 2009	✓		✓	✓		
Schotman et al. 2013	✓		✓		✓	
Bannerman 2010	✓		✓			
پژوهش حاضر	✓	✓	✓	✓		✓

بر اساس نتایج به‌دست آمده از این پژوهش، مشخص شد که تفاوت قابل ملاحظه‌ای در اهمیت ریسک‌های هر دو نوعِ محسوس و نامحسوس وجود دارد. خبرگان ریسک‌های نامحسوس (با وزن نهایی ۰/۸۶۵) را بسیار مهم‌تر از ریسک‌های محسوس (با وزن نهایی ۰/۱۳۵) دانسته‌اند. این امر، لزوم توجه ویژه به ریسک‌های نامحسوس و برنامه‌ریزی برای مقابله با آنها را نشان می‌دهد. همچنین، در این پژوهش میزان اهمیت هر یک از ریسک‌های مرتبط با دو گروه محسوس و نامحسوس نیز مشخص شده است. ریسک

«محرمانگی داده» (با وزن نهایی ۰/۲۸۷) از گروه نامحسوس به‌عنوان مهم‌ترین ریسک در به‌کارگیری رایانش ابری در سازمان‌های دولتی قلمداد شده است. پس از آن «حفاظت از داده» با اختلاف کم، مهم‌ترین ریسک شناخته شده است. پس از آن «مکان داده» با فاصلهٔ بیشتری از «حفاظت داده» در جایگاه سوم به‌لحاظ اهمیت قرار گرفت. در جدول شماره ۶، وزن نهایی هر ریسک به‌طور جداگانه آورده شده است. بنابراین، واضح است که مسائل مربوط به محرمانگی و حفاظت داده از مهم‌ترین ریسک‌هایی می‌باشند که سازمان‌ها با آن درگیر هستند. به‌عبارت دیگر، سازمان‌ها نیاز دارند تا از امنیت داده‌هایشان از طرف شرکت‌های فروشندهٔ خدمات ابر، مطمئن شوند. از این‌رو در گام اول، استفاده از خدمات شرکت‌های داخلی که مطمئن و با سابقه هستند، پیشنهاد می‌گردد.

۵. پیشنهادها

معرفی هر فناوری جدید به سازمان، ریسک‌های بسیاری در ارتباط با پیاده‌سازی و استفاده از آن فناوری را به ارمغان می‌آورد. بنابراین، بسیار مهم است که نه‌تنها باید ریسک‌های مرتبط با هر فناوری جدید یا پیاده‌سازی‌شده را شناسایی کرد، بلکه باید یک استراتژی که به سازمان‌ها کمک کند تا ریسک‌ها را بهتر مدیریت کنند و آنها را کاهش دهند، تنظیم شود. توصیه می‌شود که قبل از امضای اولین قرارداد، یک برنامهٔ مدیریت ریسک مناسب وجود داشته باشد، به‌گونه‌ای که بتواند به‌طور فعال و مستمر ریسک‌های فناوری و سیستم‌ها را شناسایی، کنترل، ارزیابی و مدیریت کند تا از وقوع آنها جلوگیری کرده یا اثراتشان را کاهش دهد.

بحث دیگر دربارهٔ به‌کارگیری فناوری رایانش ابری در سازمان‌های دولتی، بحث حاکمیتی است. با توجه به نبودِ سیاست‌های توسعه‌یافته و اثبات‌شده راجع به محیط ابری در سازمان‌های دولتی، این سؤال پیش می‌آید که آیا سازمان‌های دولتی می‌توانند به‌طور موفقیت‌آمیزی ریسک‌های کار در محیط ابری را شناسایی و مدیریت کنند؟ و یا تا قبل از اینکه سیاست‌ها، استانداردها، و مهارت‌های فنی تصویب شوند و به آنها کمک کنند که از بروز ریسک های ناخواسته جلوگیری کنند، با احتیاط پیش بروند؟

موضوع کلیدی، بحث حاکمیتی و سیاست‌گذاری است. سازمان فناوری اطلاعات ایران باید مکانیزمی جهت شناسایی، ارزیابی، و کاهش‌دادن ریسک‌های به‌کارگیری

رایانش ابری در سازمان‌های دولتی ایجاد کند. ساختار سیاست‌گذاری فناوری اطلاعات در سازمان‌های دولتی باید زیرِ چتر سازمان فناوری اطلاعات فعالیت داشته باشد. باید توجه داشت که اگرچه سازمان فناوری اطلاعات قادر به سیاست‌گذاری و کنترل موارد فناوری اطلاعات در سازمان‌های دولتی است، چالش اصلی، مدیریت و کنترل ارائه‌دهندگان رایانش ابری در خارج از دولت می‌باشد. این امر مستلزم یک «توافق در سطح خدمات»[1] قوی و درک کامل و درستی از ریسک‌های رایانش ابری می‌باشد.

برای اینکه سازمان فناوری اطلاعات توانایی شناسایی ریسک‌ها برای فناوری‌های ابری را داشته باشد و آن فناوری‌ها را درون فناوری اطلاعات سازمان‌ها (بدون اینکه آنها در معرض ریسک‌های پیش‌بینی‌نشده و ناخواسته قرار گیرند)، پیاده‌سازی نماید، بایستی یک ساختار حاکمیتی مناسب تهیه شود تا بر برنامهٔ مدیریت ریسک نظارت کند. این برنامه، سیاست‌های در نظر گرفته‌شده برای کاهش ریسک‌های محسوس و قابل درک به‌کارگیری رایانش ابری، و آن ریسک‌های نامحسوسی را که مختص عملیات سازمان‌های دولتی و اثرگذار بر شهروندان است، مدیریت می‌کند. بدون وجود سطح مناسبی از نظارت و مدیریت، پیاده‌سازی زیرساخت‌های ابر و نگران‌شدن از عواقب بعد از آن، به عواقب غیرقابل پیش‌بینی و نامطلوب نسبت به اطلاعات سازمان‌ها منجر می‌شود.

یکی از موارد مهمی که نتایج یک پژوهش علمی را برجسته‌تر می‌کند، مقایسه و مقابلهٔ آن با پژوهش‌های مشابه است. همان‌طور که جدول شماره ۸ نشان می‌دهد، این پژوهش تنها پژوهشی است که در آن ریسک‌ها توسط خبرگان شناسایی و رتبه‌بندی شده‌اند، اما به‌دلیل عدم وجود پژوهش‌های مشابه، امکان مقابله و مقایسهٔ نتایج از محققان گرفته شده است، و این، یکی از محدودیت‌های مهم این پژوهش به شمار می‌رود.

از آنجا که این پژوهش عوامل ریسک رایانش ابری در سازمان‌های دولتی را بررسی کرده، احتمال می‌رود که نتایج آن قابل تعمیم به شرکت‌های خصوصی نباشد. در این راستا، برای پژوهش‌های آینده پیشنهاد می شود که همین موضوع در بخش خصوصی مورد مطالعه قرار گیرد. همچنین، برای تحقیقات آینده توصیه می‌شود، راهکارهای مناسبی جهت مدیریت دقیق ریسک‌هایی که در این پژوهش شناسایی و اولویت‌بندی شده‌اند،

1. services level agreement (SLA)

ارائه گردد. محققان با انجام مطالعات گسترده در این زمینه و ارائهٔ دیدگاه‌ها و نظرات موشکافانهٔ خود می‌توانند یاریگر سازمان‌ها باشند.

٦. فهرست منابع

آذر، عادل، و حجت فرجی. ۱۳۸۹. *علم مدیریت فازی*. تهران: انتشارات مهربان.

زنجیرچی، سید محمود. ۱۳۹۰. *فرایند تحلیل سلسله‌مراتبی فازی*. تهران: صانعی شهمیرزادی.

Avram, G. 2014. *Advantages and challenges of adopting cloud computing from an enterprise perspective*. Proceedings of the 7th International Conference Interdisciplinarity in Engineering, Procedia Technology 12: 529–534.

Bannerman, Paul L. 2010. *Cloud Computing Adoption Risks: State of Play*. Asia Pacific Software Engineering Conference (APSEC 2010), Cloud Workshop.

Bermbach, D., M. Klems, S. Tai, and M. Menzel. 2011. *Metastorage: A federated cloud storage system to manage consistency-latency tradeoffs*. in Cloud Computing (CLOUD), IEEE International Conference 452-459.

Brender, N., and I. Markov. 2013. Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International Journal of Information Management* 33 (5): 726–733.

Briscoe, G., and A. Marinos. 2009. *Digital ecosystems in the clouds: towards community cloud computing*. 3rd IEEE International Conference on Digital Ecosystems and Technology. 103-108.

Carroll, M, van der Merwe, and P. Kotzé. 2011. *Secure cloud computing: Benefits, risks and controls*. Paper presented at the 10th Annual Information Security for South Africa (ISSA) Conference Johannesburg, South Africa.

Colt. 2011. *European CIO Cloud Survey*. Colt. May.

Craig, R, J. Frazier, N. Jachnis, S. Murphy, C. Purcell, and P. Spencer. 2009. *Cloud Computing in the Public Sector: Public Manager's Guide to Evaluating and Adopting Cloud Computing.* Cisco Internet Business Solutions Group (IBSG).

Cunningham, P. 2009. Three cloud computing risks to consider. *Information security magazine*. Retrieved from http://www.arma.org/press/armanews/infosecurity.pdf

Doherty, E., M. Carcary, and G. Conwa.2012. Risk Management Considerations in Cloud Computing Adoption. Innovation Value Institute, Executive Briefing, Retrieved from: eprints.nuim.ie/4302/1/GC_Cloud_Computiong_Adoption.pdf

Gomolski, B. 2005. *US IT spending and Staffing Survey* Gartner Research.

Grobauer, B, T. Walloschek, and E. Stocker. 2011. Understanding cloud computing vulnerabilities. *IEEE Security & Privacy* 9 (2): 50-57.

Heiser, J., and M. Nicolett. 2008. *Assessing the security risks of cloud computing.* Stamford, CT: Gartner Research. Retrieved from. http://cloud.ctrls.in/files/assessing-the-security-risks.pdf

Kaufman, L. M. 2009. Data security in the world of cloud computing. *IEEE Security and Privacy* 7 (4): 61–64.

Kwong, C. K., and H. A Bai. 2002. Fuzzy AHP approach to the determination of importance weights of customer requirements in quality function deployment. *Journal of Intelligent Manufacturing* 13 (5): 367-377.

Lian, J, D. Yen, and Y. Wang. 2013. An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management* 34 (1): 28-36.

Mahmood, Z. 2011. *Data Location and Security Issues.*In Cloud Computing. International Conference on Emerging Intelligent Data and Web Technologies (EIDWT) 49-54.

Mell, P, and T. Grance. 2011. The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology Retrieved from. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Paquette, S, P. Jaeger, and S. Wilson. 2010. Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly* 27 (3): 245–253.

Percin, S. 2008. Use of fuzzy AHP for evaluating the benefits of information sharing decisions in a supply chain. *Journal of Enterprise Information Management* 21 (3): 263-284.

Saaty, T. L. 1989. *Group decision making and the AHP*. New York: Springer.

Schotman, R, A. Shahim, and A. Mitwalli. 2013. *Cloud Risks - Are we looking in the right direction?* The open cloud company (CANOPY).

Shahzad, F. 2014. State-of-the-art Survey on Cloud Computing Security: Challenges, Approaches and Solutions. Proceedings of the 5th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2014). *Procedia Computer Science* 37: 357–362.

Subashini, S., and V. Kavitha. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* 34 (1): 1–11.

Sultan, N. 2010. Cloud computing for education: A new dawn? *International Journal of Information Management* 30 (2): 109-116.

_____. A. 2011. Reaching for the cloud: How SMEs can manage. *International Journal of Information Management* 31 (3): 272–278.

Tribhuwan, M, V. Bhuyar, and S. Pirzade. 2010. *Ensuring Data Storage Security in Cloud Computing through Two-Way Handshake Based on Token Management.* International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom): 386-389.

Wei, L, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. Vasilakos. 2013. Security and privacy for storage and computation in cloud computing. *Information Sciences* 258: 371-386.

Whitman, M, and H. Mattord. 2010. *Management of information security*. Course Technology Ptr.

Wyld, D. 2009. Moving to the cloud: an introduction to cloud computing in governmentE-

Government Series. IBM Center for the Business of Government. Retrieved from. www.businessofgovernment.org.

Zhou, M., R. Zhang, W. Xie, W. Qian, and A. Zhou. 2010. *Security and privacy in cloud computing: A survey*. In Semantics knowledge and grid (SKG), 2010 sixth international conference on 1–3 November.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی